

UNITED STATES DISTRICT COURT

for the
District of Oregon

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*The Phone and Digital Media, currently located at Salem
Police Department, as described in Attachment A

Case No.

'19 -MC-1024

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The Phone and Digital Media as described in Attachment A hereto,

located in the _____ District of _____ Oregon _____, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

21 U.S.C. 841(a)(1)

Possession with Intent to Distribute Methamphetamine

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Applicant's signature

ROLAND JACOBS, Special Agent, ATF

Printed name and title

Sworn to before me and signed in my presence.

Date:

Nov. 26, 2019


 Judge's signature

City and state: Portland, Oregon

STACIE F. BECKERMAN, United States Magistrate Judge

Printed name and title

ATTACHMENT A

Phone and Digital Media to Be Searched

1. One gold Samsung cellular telephone, model SM-J727T1, serial number J727T1UVU1AQG1 (the Phone) associated with Salem Police Department case number SMP19012533, evidence item # 6Q.



2. One (1) memory card and three (3) AT&T Prepaid Nano (SIM) cards (Digital Media) associated with Salem Police Department case number SMP19012533, evidence item #7Q.



Both items 6Q and 7Q are currently stored at Salem Police Department located at 555 Liberty Street SE, Salem, Oregon.

ATTACHMENT B

Items to Be Seized

1. All records on the Phone and Digital Media described in Attachment A that relate to violations of 21 U.S.C. § 841(a)(1) and involve Donald Gordon SAGER between April 4, 2018 to April 4, 2019, including:
 - a. Evidence relating to illegal possession and distribution of methamphetamine.
 - b. Types, amounts, and prices of methamphetamine possessed and sold, as well as dates, places, and amounts of specific transactions.
 - c. Information related to the sources and users of methamphetamine (including names, addresses, phone numbers, or any other identifying information).
 - d. Bank records, checks, credit card bills, account information, and other financial records indicating purchases or sales of methamphetamine.
 - e. Lists of customers and related identifying information.
2. Evidence of user attribution showing who used or owned the Phone and Digital Media at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.
3. Records evidencing the use of the Internet, including:
 - a. Records of Internet Protocol addresses used.
 - b. Records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

c. Records of data storage accounts and use of data storage accounts.

4. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Search Procedure

5. The examination of the Phone and Digital Media may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Phone and Digital Media to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the Phone and Digital Media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Phone, Digital Media or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the

operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the Phone or Digital Media does not contain any data falling within the ambit of the warrant, the government will return the Phone and Digital Media to its owner within a reasonable period of time following the search and will seal any image of the Phone and Digital Media, absent further authorization from the Court.

9. The government may retain the Phone and Digital Media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Devices and/or the data contained therein.

10. The government will retain a forensic image of the Phone and Digital Media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

DISTRICT OF OREGON, ss: AFFIDAVIT OF ROLAND JACOBS

**Affidavit in Support of an Application
for a Search Warrant for a Phone and Digital Media**

I, Roland Jacobs, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives, and have been for over 28 years. My current assignment is to the Portland, Oregon Field Office. I have attended and completed the Criminal Investigator School and the ATF New Agent Training School at the Federal Law Enforcement Training Center in Glynco, Georgia. As an ATF Special Agent, I am charged with the responsibility of enforcing Federal firearms laws of the United States. I have participated in investigations involving firearms trafficking, National Firearms Act violations, unlawful firearms possession, and illegal narcotic trafficking, which often involves firearms. I have participated in investigations where the use of computers, cellular phones, digital media, and the internet have been used in furtherance of crimes related to the illegal possession and trafficking of firearms and narcotics.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of a gold Samsung cellular telephone, model SM-J727T1, serial number J727T1UVU1AQQ1 (hereinafter Phone), as well as one memory card, and three AT&T prepaid NANO (SIM) cards (hereinafter collectively referred to as Digital Media), which are currently in evidence at the Salem Police Department (SPD), located at 555 Liberty Street SE, Salem, Oregon associated with SPD Case # SMP19012533 items 6Q and 7Q, as described in Attachment A hereto, and the extraction of electronically stored information from the Phone and Digital Media, as described in

Attachment B hereto. As set forth below, I have probable cause to believe and do believe that the items set forth in Attachment B constitute evidence, fruits and instrumentalities of violations of 21 U.S.C. § 841(a)(1).

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. Title 21, United States Code, Section 841(a)(1) makes it unlawful for any person to knowingly or intentionally manufacture, distribute, or possess with intent to distribute a controlled substance (Methamphetamine).

Statement of Probable Cause

5. In April 2019, I became involved in a state investigation regarding the possession of methamphetamine by DONALD GORDON SAGER (DOB: XX/XX/1953). SAGER has multiple prior felony convictions and was on post-prison supervision when he was arrested on April 4, 2019. I reviewed Marion County Parole and Probation (MCP) Officer Juster's report and SPD Officer Basaraba's Crime/Incident report #SMP19012533 describing SAGER's arrest, and summarized the reports below.

6. On April 4, 2019, at approximately 3:37 p.m., MCPP Officers Juster and Gomez were in the area of 650 Locust Street NE, Salem, Oregon, when they recognized a vehicle associated with SAGER. MCPP Juster supervises SAGER on post-prison supervision, and he requested and obtained a parole violation warrant for SAGER on April 1, 2019. MCPP Officers Juster and Gomez set up surveillance on the vehicle and within minutes saw SAGER approach the vehicle. MCPP Officers Juster and Gomez contacted SAGER and arrested him.

7. While searching SAGER incident to arrest, MCPP Officer Juster recovered four (4) plastic baggies of a white crystal like substance, one gold Samsung cellular telephone, one memory card, a Samsung adapter, three AT&T prepaid NANO (SIM) cards, a black/white handkerchief, a red plastic straw, and \$93. MCPP Juster contacted SPD Officer Basaraba, who arrived at SAGER's arrest scene. SPD Officer Basaraba advised SAGER of his rights and asked SAGER about the white crystal like substance MCPP Juster found. SAGER admitted to Officer Basaraba that the substance was methamphetamine. Officer Basaraba field tested a portion of one of the four baggies, and it tested positive for methamphetamine. The four plastic baggies were later submitted to Oregon State Police Forensic Laboratory for quantitative analysis, and found to contain 72.63 grams of actual methamphetamine.

8. On April 11, 2019, Donald Gordon SAGER was indicted by a federal grand jury for one count of Possession with the Intent to Distribute Methamphetamine, in violation of Title 21 United States Code, Sections 841(a)(1) and 841(b)(1)(B), case 3:19-cr-00131-MO.

9. Based on my training and experience I know people involved in the unlawful purchase and distribution of narcotics often communicate with others in order to facilitate their illegal activities. This communication often takes place between the seller and purchaser of

narcotics, who use cell phones to facilitate the sale of narcotics. I know people involved in narcotics distribution often document their possession and use of narcotics via videos, pictures, and messages on their cellular phones and other digital media. I also know people involved in narcotics distribution often use multiple cell phones or “burner” phones to conceal their illegal activity from law enforcement.

10. The Phone and Digital Media are currently in the lawful possession of the Salem Police Department (SPD), located at 555 Liberty Street SE, Salem, Oregon. They came into SPD’s possession when they were seized incident to arrest.

11. The Phone and Digital Media are currently in storage at SPD in evidence associated with SPD Case # SMP19012533 items 6Q and 7Q. In my training and experience, I know that they have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when they first came into the possession of SPD.

12. Based on my training and experience, a wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video;

recording, storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet,¹ including the use of apps.² Wireless telephones may also include a global positioning system (“GPS”) technology for determining the location of the device.

13. Based on my training, experience, and research, I know that the Phone has capabilities that allow it to serve as wireless telephone, digital camera, and portable media player, GPS, and can provide internet access. In my training and experience, examining data stored on wireless telephones and digital media can uncover, among other things, evidence that reveals or suggests who possessed or used the phone, how the phone was used, and the purpose of its use.

14. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the phone was used, the purpose of its use, who used it, and when. There is probable cause to believe this forensic electronic evidence will be on the phone and digital storage devices because, based on my knowledge, training, and experience, I know:

- a. Phones and Digital Media can store information for long periods of time,

¹ The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

² Apps is an abbreviation for applications. An app is a self-contained program or piece of software designed to fulfill a particular purpose. An app can run on the Internet, on a computer, on a cell phone, or on other electronic devices.

including information viewed via the Internet. Files or remnants of files can be recovered with forensic tools months or even years after they have been downloaded onto a phone, deleted, or viewed via the Internet. Electronic files downloaded to a phone can be stored for years at little or no cost. When a person “deletes” a file, the data contained in the file does not actually disappear, rather that data remains on the phone until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the phone that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, the operating system may also keep a record of deleted data.

b. Wholly apart from user-generated files, the Phone may contain electronic evidence of how it has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, and file system data structures.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

d. Data on the Phone can provide evidence of a file that was once on the phone but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Systems can leave traces of information on the Phone that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the phone that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, including SD cards or other flash media, and

the times the phone was in use. File systems can record information about the dates files were created and the sequence in which they were created.

e. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

f. A person with appropriate familiarity with how the Phone works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how the phone was used, the purpose of its use, who used it, and when.

g. The process of identifying the electronically stored information necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on the Phone is evidence may depend on other information stored on the phone and the application of knowledge about how a phone functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

h. Further, in order to find evidence of how the Phone was used, the purpose of its use, who used it, and when, the examiner may have to establish that a particular thing is not present on the phone.

15. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Phone and Digital Media consistent with the warrant. The examination may require authorities to employ techniques, including imaging the Phone and computer-assisted scans and searches of the Phone

that might expose many parts of the device to human inspection in order to determine whether it constitutes evidence as described by the warrant.

16. The initial examination of the Phone and Digital Media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

17. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Phone, Digital Media or image extracted do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

18. If an examination is conducted, and it is determined that the Phone or Digital Media does not contain any data falling within the ambit of the warrant, the government will return the Phone or Digital Media to its owner within a reasonable period of time following the search and will seal any image of the Phone, absent further authorization from the Court.

19. The government may retain the Phone and Digital Media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the

phone and/or the data contained therein.

20. The government will retain a forensic image of the Phone and Digital Media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

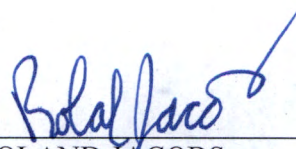
21. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

22. Based on the foregoing, I have probable cause to believe, and I do believe, that the Phone and Digital Media contain evidence, fruits and instrumentalities of violations of; Title 21 U.S.C. § 841(a)(1), possession with intent to distribute methamphetamine, as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the Phone and Digital Media for the items listed in Attachment B and the seizure and examination of any such items found.

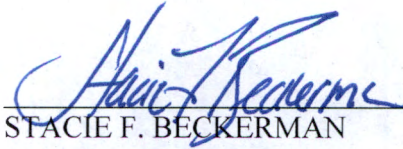
23. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Hannah Horsley, and AUSA Horsley advised me that in her opinion the

affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.



ROLAND JACOBS
ATF Special Agent

Subscribed and sworn to before me this 26th day of November, 2019.



STACIE F. BECKERMAN
United States Magistrate Judge